ABSTRACT

FULLY SECURE MESSAGE TRANSMISSION OVER NON-SECURE CHANNELS WITHOUT CRYPTOGRAPHIC KEY EXCHANGE

A cryptographic system transmits a fully secure cryptographic message over a non-secure communication channel without prior exchange of cryptographic keys using a three-pass protocol. The transmitting agent initiating the communication embodies the message for the designated receiving agent in the composite output of two distinct transformations such that a generalized reversal of the combined transformations cannot be determined from that output. That output is transmitted as a first-pass over a non-secure channel to the receiving agent. The receiving agent generates a second composite output by transforming the received message such that a generalized reversal of this second combined transformation cannot be determined from that resulting output. That second output is transmitted as a second-pass over a non-secure channel to the initial transmitting agent. The initial agent generates a third composite output from the returned message by reversing one of the two initial transformations such that a generalized reversal of this third composite transformation cannot be determined from that resulting output. The third output is transmitted as a third-pass over a non-secure channel to the receiving agent. The receiving agent uses a reversal of the second transformation applied to the final message to extract the initial message. The transformations (or keys) used by either party need not be known by the other, making this an independent-key cryptographic process. It is technically impossible for any eavesdropping agent, even one who captures

all transmissions between the transmitting and receiving agents, to directly recreate the initial message from the observed transmissions.